MICHAEL F. RAM (SBN 104805)
mram@forthepeople.com
MARIE N. APPEL (SBN 187483)
mappel@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 358-6913
Telephone: (415) 358-6293

JOHN A. YANCHUNIS (*Pro Hac Vice*)
jyanchunis@forthepeople.com
RA O. AMEN (*Pro Hac Vice*)
ramen@ forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin St., 7th Floor
Tampa, FL 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

KYLE ALLEN BANTA YOSHIDA, an individual and California resident, on behalf of himself and all others similarly situated,

Plaintiff,

vs.

BACKROADS, a California corporation.

Defendant.

Case No.:

CLASS ACTION COMPLAINT

1) Negligence;

2) Declaratory Relief;

3) Violation of the California Unfair Competition Law, Code § 17200, *et seq.* – Unlawful Business Practice;

4) Violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq.*;

5) Breach of Implied Contract; and

6) Breach of Confidence

DEMAND FOR JURY TRIAL

Plaintiff Kyle Allen Banta Yoshida brings this Class Action Complaint against Backroads, a California corporation, ("Backroads" or "Defendant"), on behalf of himself and all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Founded in 1979, Backroads is an adventure travel company, offering packaged international adventure trips such as biking tours, walking and hiking trips, family adventures, and multi-sport trips, as well as travel support, tips, and reviews.

2. On or about November 19, 2020, Backroads notified its employees and former employees, and state Attorneys General about a data breach occurring in or around October 2020, which it initially detected on October 2, 2020, (hereinafter "the Data Breach" or "the Breach").

3. The Data Breach involved employees' and former employees' "name, date of birth, Social Security number, government issued ID (passport or driver's license, if provided to Backroads), financial account information and health insurance information, if obtained through Backroads." Backroads Notice of Data Breach, attached as Exhibit A, *available at* https://media.dojmt.gov/wp-content/uploads/Backroads-Notif.pdf.

4. As a matter of course, and on an ongoing basis, Backroads collected its employees' sensitive personal and financial information, including names, addresses, Social Security numbers, bank account numbers, and other personal and financial information ("Personal Information") as a condition of their employment. Accordingly, Backroads had an obligation to secure that information by implementing reasonable and appropriate safeguards compliant with industry-standard data security practices.

5. As a result of Backroads' failure to protect the information with which it was entrusted to safeguard, Plaintiff and Class members have already suffered harm and have been exposed to a significant risk of identity theft, financial fraud, and other identity-related fraud for years to come.

6. This Personal Information was compromised due to Backroads' negligent and/or careless acts and omissions and the failure to protect employees' and former employees' data.

7. The stolen Personal Information has great value to hackers due to the numbers involved: It is likely that thousands of people – residents of many states – were affected by this Breach.

8. Plaintiff brings this action on behalf of all persons whose Personal Information was compromised as a result of Defendant's failure to: (i) adequately protect its employees' and former employees' Personal Information, (ii) warn employees and former employees of its inadequate information security practices, and (iii) effectively monitor its information systems for security vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates several California statutes.

9. Plaintiff and similarly situated Backroads' employees and former employees ("Class members") have suffered injury as a result of Defendant's conduct. These injuries may include: (i) lost or diminished value of Personal Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) deprivation of rights they possess under the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200), the California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq*.); and (v) the continued and certainly an increased risk to their Personal Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information.

II. PARTIES

10. Plaintiff Kyle Allen Banta Yoshida is a citizen of California residing in Oakland. Plaintiff Banta Yoshida worked for Backroads from approximately July 2017 to September 2018, as a systems administrator, reporting to the Director of Information Technology. He received Backroads' notice of the Data Breach, dated November 19, 2020, or shortly thereafter.

11. Defendant Backroads is a California corporation with its principal place of business located at 801 Cedar Street, Berkeley, California 94710. During the class period,

Backroads operated in California through its physical location and website.

III. JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

13. This Court has jurisdiction over Defendant as it maintains its corporate headquarters in this District. Defendant is authorized to and conducts business in this District and is subject to general personal jurisdiction in this state.

14. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, Backroads maintains its headquarters within this District, and Backroads has caused harm to Class members residing in this District.

IV. FACTUAL ALLEGATIONS

15. Backroads is a high-end, adventure travel company. Backroads describes itself as the "the world's #1 active travel company": set apart by its:

> meticulous trip design[, . . .] elegant hotels and world-class dining. And our Trip Leaders, who are consistently described by our guests as the best guides they've ever had. Backroads sets the benchmark for incredible biking, hiking and multi-adventure trips worldwide. Never subcontracted, in more than 65 countries and with more dates to choose from than any other company.[1]

16. Backroads employs more than 200 office/warehouse staff, and has a team in the field, consisting of over 800 Trip Leaders, Camp Chefs and Camp Assistants, spread across 58 countries.

17. Backroads was aware of its need to protect the information of its customers and employees. Specifically, the Backroads Privacy Policy:

[1] Backroads, *About Backroads*, https://www.backroads.com/about (last visited December 16, 2020).

> sets out how we obtain, store and use your personal information when you use or interact with www.backroads.com or my.backroads.com (our web sites), or where we otherwise obtain or collect your personal information. By using any of our web sites or sharing your personal information with us, you are accepting and consenting to the practices described in this Privacy Policy.[2]

18. The Backroads Privacy Policy notes that its "relationship with you is very important to us" and Backroads is "sensitive to protecting the private information that you provide to us." Further, "Backroads ensures 3rd Party contracts contains proper controls for: anonymize and encryption of personal data, breach detection, and deletion of personal data at the end of contract term." *Id.* Finally, in the Privacy Policy, Backroads agrees that:

> Except as otherwise described in this privacy statement, Backroads will not disclose personal information to any third party unless we believe that disclosure is necessary:
> - To conform to legal requirements or to respond to a subpoena, search warrant or other legal process received by Backroads, whether or not a response is required by applicable law
> - To enforce the Backroads Terms of Service Agreement or to protect our rights
> - To protect the safety of members of the public and users of the service.

Id.

19. At all relevant times, Backroads was aware, or should have been aware, that the Personal Information it collected, maintained and stored in its systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud. Indeed, Backroads undoubtedly observed frequent public announcements of employee-related data breaches affecting technology companies, healthcare companies, retailers, and restaurant chains and knew that personal and financial information of the type stored by Backroads is highly coveted and a frequent target of hackers.

20. The widely-known rise in the number of data breaches is attributable to the fact that information of the type exposed in the Data Breach is highly-coveted and valuable on underground markets. For example, a cyber "black market" exists in which criminals openly post

[2] Backroads, *Backroads Privacy Policy*, https://www.backroads.com/privacy (last visited December 16, 2020).

and sell stolen consumer information on underground internet websites known as the "dark web" – exposing impacted individuals to identity theft and fraud for years to come.

21. Legitimate organizations and the criminal underground alike recognize the value of personal information contained in an employer's data systems; otherwise, they would not aggressively seek or pay for it. At all relevant times, Backroads knew, or reasonably should have known, of the importance of safeguarding the Personal Information and of the foreseeable consequences of a breach of its data security system, including, specifically, the significant costs that would be imposed on its employees as a result of a breach.

22. In this case, Backroads was at all times fully aware of its obligation to protect the Personal Information of its employees. Backroads was also aware of the significant repercussions if it failed to do so because Backroads collected data from thousands of employees and knew that this data, if hacked, would result in injury to its employees, including Plaintiff and Class members. Unfortunately, despite its recognition of the risks of inadequate data security practices, Backroads failed to adopt reasonable safeguards to protect against even known and obvious cyber-threats.

The Data Breach

23. On or about November 19, 2020, Backroads sent employees and former employees a *Notice of Data Breach*.[3] Backroads' Founder and CEO, Tom Hale, informed the recipients of the notice that:

> ***What Happened?***
> On October 2, 2020, Backroads became aware of suspicious activity within its computer network. Backroads immediately began an investigation, working with external forensic specialists, to determine the nature and scope of the activity. Our investigation determined that certain files within our environment were encrypted and inaccessible. On October 16, 2020, we discovered that certain files had been accessible to unknown actors and that certain personal information was contained in these files. [….]

[3] Backroads's *Notice of Data Breach*, November 19, 2020, archived by the Maine Attorney General, *available at*: https://apps.web.maine.gov/online/aeviewer/ME/40/96c8ab0d-a0a7-41e6-8f75-8712a56fda56/48862ef5-de5e-48c2-bceb-01fc587fa2a2/document.html (last accessed April 23, 2021).

> ***What Information Was Involved?***
> Backroads has both legal authority and obligation to maintain personal information for its employees. The forensic investigation confirmed that the following information was stored within one of the impacted network devices and may have been accessible to unknown actors: your name, date of birth, Social Security number, government issued ID (passport or driver's license, if provided to Backroads), financial account information and health insurance information, if obtained through Backroads. While we cannot confirm which piece of your personal information might have been accessed, we are informing employees of the full scope of what could have been compromised due to its presence in impacted files. [4]

24. Unfortunately, Backroads' notification to affected individuals was severely deficient in numerous respects. First, Backroads failed to disclose exactly who was affected and what information was compromised, instead using vague phrasing "personal information for its employees," and noting that it "cannot confirm which piece of your personal information might have been accessed." But employers like Backroads routinely store all sorts of other employee information, including full names and addresses, e-mail addresses, employee system passwords, tax information, W-2 and other IRS forms, insurance information that may include the personal information of dependents and family members, and payroll records, among others. Consequently, Plaintiff and Class members remain in the dark regarding what information was actually stolen.

25. Backroads' failure to specify what information was stolen is important because affected individuals may take different precautions depending on what type of information was compromised. For example, if W-2 information, tax information, or payroll records were compromised, affected individuals may need to contact the Internal Revenue Service or their accountants to place fraud alerts on their accounts. If the breach included Social Security numbers or other identifiable information, the impacted individuals may need to enroll in credit monitoring or contact their financial institutions or credit bureaus to freeze their accounts. By failing to identify exactly who was affected or what information was compromised, Backroads has prevented its current and former employees from taking meaningful, proactive, and targeted mitigation measures that could help protect them from years of financial harm.

[4] *Id.*

26. In addition to lacking the necessary safeguards to secure Personal Information, Backroads did not have adequate monitoring systems and controls in place to detect the unauthorized infiltration after it occurred. Backroads, like any company its size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to thousands of employee files.

Backroads Failed to Comply with FTC Requirements

27. Federal and State governments have established security standards and issued recommendations to temper data breaches and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[5]

28. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[6] Among other things, the guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[7]

29. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security;

[5] Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Jan. 27, 2021).

[6] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 27, 2021).

[7] *Id.*

monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[8]

30. Highlighting the importance of protecting against data breaches, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect Personal Information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[9]

31. As a modern-day company, Backroads understood, or should have understood, the risks and consequences of inadequate data security, but nevertheless operated network systems with outdated operating systems and software, failed to timely detect the hackers' presence, failed to notice the massive amounts of data that were being accessed and/or exfiltrated from its databases, or take any steps to investigate the numerous other red flags that should have warned the company about what was happening.

32. Backroads' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff's Experience

33. Plaintiff Kyle Allen Banta Yoshida is a citizen of California. Plaintiff Banta Yoshida worked for Backroads from approximately July 2017 to September 2018, as a systems administrator, reporting to the Director of Information Technology. In that role, Plaintiff Banta Yoshida raised several concerns regarding Backroads' inadequate data security practices.

34. However, as a condition of his employment, Plaintiff Banta Yoshida provided

[8] FTC, *Start With Security*, *supra* note 5.

[9] Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited July 26, 2019).

Backroads with significant amounts of his personal and financial information, including his name and address, Social Security number, bank and financial account information, insurance information, and payroll and tax information, as well as information pertaining to his beneficiaries and dependents.

35. In a letter dated November 19, 2020, Plaintiff Banta Yoshida was notified by Backroads that his Personal Information may have been compromised in the Data Breach.

36. As a result of the Data Breach, Plaintiff Banta Yoshida has spent time and effort researching the Data Breach, monitoring his financial accounts and credit monitoring services to detect potential fraud.

37. Consequently, Plaintiff Banta Yoshida lost time dealing with the issues related to the Data Breach.

38. Plaintiff Banta Yoshida suffered actual injury in the form of damages to and diminution in the value of this Personal Information—a form of intangible property that Plaintiff entrusted to Backroads for the purpose of employment with Backroads and which was compromised in and as a result of the Data Breach.

39. Plaintiff Banta Yoshida suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has concerns for the loss of his privacy.

40. Plaintiff Banta Yoshida has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Personal Information being placed in the hands of criminals.

41. Plaintiff Banta Yoshida has a continuing interest in ensuring his Personal Information, which remains in the possession of Backroads, is protected and safeguarded from future breaches.

The Data Breach Caused Harm and Will Result in Additional Fraud

42. Without detailed disclosure to Backroads' employees and others impacted, affected individuals including Plaintiff and Class members have been left exposed, unknowingly and unwittingly, for months, to continued misuse and ongoing risk of misuse of their Personal Information without being able to take necessary precautions to prevent imminent harm.

43. The ramifications of Backroads' failure to keep Plaintiff's and Class members' data secure are severe.

44. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R § 248.201. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person." *Id*.

45. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[10]

46. Identity thieves can use personal information, such as that of Plaintiff and Class members, which Backroads failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits or medical treatment; (f) file a fraudulent tax return using the victim's information; (g) commit espionage; or (h) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

47. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.

[10] Federal Trade Commission, *Warning Signs of Identity Theft* (May 2015), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Jan. 27, 2021).

> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[11]

48. The unauthorized disclosure of Social Security Numbers can be particularly damaging because Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[12]

49. In fact, Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[13]

---

[11] Federal Trade Commission, *Combating Identity Theft A Strategic Plan* (April 2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited July 26, 2019).

[12] Social Security Administration, *Identity Theft and Your Social Security Number* (June 2017), *available at*: http://www.ssa.gov/pubs/10064.html (last visited July 26, 2019).

[13] Javelin Research, *2016 Identity Fraud: Fraud Hits an Inflection Point* (Feb. 2, 2016), *available at:* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited July 26, 2019).

50. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[14]

51. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

52. Moreover, Plaintiff and Class members place significant value in data security. Had they known their employer would not adequately protect and secure their Personal Information, they would have refused to provide such information or sought alternative employment.

Plaintiff and Class Members Suffered Damages

53. The Personal Information of Plaintiff and Class members is private and sensitive in nature and was left inadequately protected by Backroads. Backroads did not obtain Plaintiff's and Class members' consent to disclose their Personal Information to any other person as required by applicable law and industry standards.

54. The Data Breach was a direct and proximate result of Backroads' failure to properly safeguard and protect Plaintiff's and Class members' Personal Information from unauthorized access, use, and disclosure, as required by various state and federal regulations,

[14] U.S. Department of Justice, *Victims of Identity Theft, 2014* (Sept. 2015, revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 26, 2019).

[15] U.S. Government Accountability Office Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited July 26, 2019).

industry practices, and the common law, including Backroads' failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' Personal Information to protect against reasonably foreseeable threats to the security or integrity of such information.

55. Backroads had the resources to prevent a breach. Backroads made significant expenditures to market its services, but neglected to adequately invest in data security, despite the growing number of intrusions and several years of well-publicized data breaches.

56. Had Backroads remedied the deficiencies in its systems, followed government guidelines, and adopted security measures recommended by experts in the field, Backroads would have prevented or discovered the intrusion into its network and systems and, ultimately, the theft of its current and former employees' Personal Information.

57. As a direct and proximate result of Backroads' wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time, which they otherwise would have dedicated to other life demands, such as work, to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports.

58. Backroads' wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' Personal Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. identity theft and fraud resulting from the theft of their Personal Information;

b. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

c. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

d. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

e. lowered credit scores resulting from credit inquiries following fraudulent activities;

f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

g. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals and/or misused via sale on the Internet black market;

h. damages to and diminution in value of their Personal Information entrusted to Backroads for the sole purpose of working for Backroads; and

i. the loss of Plaintiff's and Class members' privacy.

59. Backroads continues to hold Personal Information of its current and former employees, including Plaintiff and Class members. Particularly because Backroads has demonstrated an inability to prevent a breach, or stop one from continuing even after detection, Plaintiff and Class members have an undeniable interest in ensuring that their Personal Information is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

V. CLASS ALLEGATIONS

60. Plaintiff seeks relief on behalf of himself and as representatives of all others who are similarly situated. Pursuant to Rule 23(a), (b)(2), (b)(3) and/or (c)(4), Fed. R. Civ. P., Plaintiff seeks certification of a nationwide class defined as follows:

> All individuals residing in the United States whose Personal Information was compromised in the data breach initially disclosed by Backroads in or about November 2020 (the "Class" or "Nationwide Class").

61. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff asserts claims under the law of California on behalf of a separate statewide subclass, defined as follows:

> All individuals residing in California whose Personal Information was compromised in the data breach initially disclosed by Backroads in or about November 2020 (the "California Subclass").

62. Excluded from the Classes are Backroads and its parents, subsidiaries, affiliates, officers and directors, and any entity in which Backroads has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

63. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

64. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Backroads has identified thousands of consumers whose Personal Information may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendant's records.

65. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class members. These include:

a. Whether Backroads had a duty to protect Personal Information;

b. Whether Backroads knew or should have known of the susceptibility of its systems to a data breach;

c. Whether Backroads' security measures to protect its systems were reasonable in light of known legal requirements, such as the FTC data security recommendations, and industry standards;

d. Whether Backroads was negligent in failing to implement reasonable and adequate security procedures and practices;

e. Whether Backroads' failure to implement adequate data security measures allowed the breach of its data systems to occur;

f. Whether Backroads' conduct constituted unfair or deceptive trade practices;

g. Whether Backroads' conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the Personal Information of Plaintiff and Class members;

h. Whether Plaintiff and Class members were injured and suffered damages or other losses because of Backroads' failure to reasonably protect its systems and data network; and,

i. Whether Plaintiff and Class members are entitled to relief.

j. Whether Backroads adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

k. Whether Backroads caused Plaintiff and Class members damages;

l. Whether Backroads violated California's Deceptive and Unfair Trade Practices Act by failing to implement reasonable security procedures and practices; and,

m. Whether Backroads violated California's California Consumer Privacy Act by failing to maintain reasonable security procedures and practices.

66. **Typicality**: Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff is a former employee whose Personal Information was in Backroads' possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to other Class members and Plaintiff seeks relief consistent with the relief of the Class.

67. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class members. Plaintiff's Counsel are competent and experienced in litigating privacy-related class actions.

68. **Superiority and Manageability**: Under 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual Class

member are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims.

69. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Backroads has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

70. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Backroads owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Backroads breached that duty;

c. Whether Backroads' security measures to protect is systems were reasonable in light of known legal requirements, such as the FTC data security recommendations, and industry standards;

d. Whether Backroads failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiff and the Class members; and,

e. Whether adherence to FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach;

f. Whether Class members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Backroads' wrongful conduct.

\\\

\\\

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class, or, Alternatively, Plaintiff and the California Subclass))

71. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 70.

72. Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, using, and protecting their Personal Information from unauthorized third parties.

73. The legal duties owed by Defendant to Plaintiff and Class members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Personal Information of Plaintiff and Class members in its possession;

b. To protect Personal Information of Plaintiff and Class members in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the data breach.

74. In addition, Cal. Civ. Code § 1798.81.5 requires Defendant to take reasonable steps and employ reasonable methods of safeguarding the Personal Information of Class members who are California residents.

75. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practices of failing to use reasonable measures to protect Personally Identifiable Information ("PII")—such as the Personal Information here—by companies such as Defendant.

76. Various FTC publications and data security breach orders further form the basis

of Defendant's duty.[16] Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with industry standards.

77. Defendant breached its duties to Plaintiff and Class members. Defendant knew or should have known the risks of collecting and storing Personal Information and the importance of maintaining secure systems.

78. Plaintiff and members of the Class entrusted Defendant with their Personal Information on the premise and with the understanding that Defendant would safeguard their information, and Defendant was in a position to protect against the harm suffered by Plaintiff and members of the Class as a result of the Data Breach.

79. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Personal Information. Defendant's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard data security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

80. Defendant knew, or should have known, of the risks inherent in collecting and storing Personal Information, the vulnerabilities of its systems, and the importance of adequate security. Defendant knew about numerous, well-publicized data breaches.

81. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Personal Information of Plaintiff and Class members.

82. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the Personal Information of Plaintiff and the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Personal

[16] *See, e.g., Data Protection: Actions taken by Equifax and Federal Agencies in Response to the 2017 Breach*, UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE (Aug. 30, 2019), *available at*: https://www.gao.gov/products/GAO-18-559 (regarding the Equifax data breach) (last accessed April 23, 2020).

Information during the period it was within Defendant's possession and control.

83. Defendant had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' willingness to entrust Defendant with their Personal Information as a condition of employment was predicated on the understanding that Defendant would take adequate security precautions.

84. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class members' Personal Information and promptly notify them about the Data Breach.

85. Defendant breached the duties it owes to Plaintiff and Class members in several ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Personal Information of Plaintiff and Class members;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class members' Personal Information both before and after learning of the Data Breach;

d. by failing to comply with industry standard data security standards during the period of the Data Breach; and

e. by failing to timely and accurately disclose that Plaintiff's and Class members' Personal Information had been improperly acquired or accessed.

86. Due to Defendant's conduct, Plaintiff and Class members are entitled to credit monitoring. Credit monitoring is reasonable here. The Personal Information taken can be used towards identity theft and other types of financial fraud against the Class members. Hackers stole everything needed to commit identity fraud. There is no question that this Personal Information was taken by sophisticated cybercriminals, increasing the risks to the Class members. The consequences of identity theft are serious and long-lasting. There is a benefit to early detection

and monitoring.

87. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $329 per year.

88. As a result of Defendant's negligence, Plaintiff and Class members suffered injuries that may include: (i) the lost or diminished value of Personal Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the continued risk to their Personal Information, which remains in Defendant's possession, subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information of employees and former employees in its continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Personal Information compromised as a result of the data breach for the remainder of the lives of Plaintiff and Class members, including ongoing credit monitoring.

89. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendant's negligent conduct.

COUNT II
Declaratory Judgment
(On Behalf of Plaintiff and the Nationwide Class)

90. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 70.

91. Defendant owes duties of care to Plaintiff and Class members that require it to adequately secure Personal Information .

92. Defendant still possess Personal Information regarding Plaintiff and Class

members.

93. Although Defendant claims it is "rebuilding our network from the ground up, and adding further security measures, to better protect against similar incidents in the future,"[17] there is no detail on what, if any, fixes have really occurred.

94. Plaintiff and Class members are at risk of harm due to the exposure of their Personal Information and Defendant's failure to address the security failings that lead to such exposure.

95. There is no reason to believe that Defendant's security measures are any more adequate than they were before the breach to meet Defendant's contractual obligations and legal duties, and there is no reason to think Defendant has no other security vulnerabilities that have not yet been knowingly exploited.

96. Plaintiff, therefore, seeks a declaration that (1) Defendant's existing security measures do not comply with its explicit and implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) Defendant must comply with its explicit and implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment Personal Information by, among other things,

[17] See Notice of Data Breach, supra note 3.

creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant conduct regular database scanning and securing checks;

f. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner Personal Information not necessary for its provisions of services; and

h. Ordering Defendant to purchase credit monitoring services for Plaintiff and Class members for a period of ten years.

COUNT III
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200 – Unlawful Business Practices
(On Behalf of Plaintiff and the Nationwide Class Or, in the Alternative, On Behalf Plaintiff and the California Subclass)

97. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 70.

98. Defendant has violated Cal. Bus. and Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Nationwide Class or, in the alternative, the California Class.

99. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and Nationwide and California Class members' Personal Information with knowledge that the information would not be adequately protected; and by storing Plaintiff's and the Nationwide and California Class members' Personal Information in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to implement and maintain reasonable security

procedures and practices to safeguard the Personal Information of Plaintiff and the Nationwide and California Class members.

100. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and the Nationwide and California Class members were injured and lost money or property, including but not limited to the loss of Nationwide and California Class members' legally protected interest in the confidentiality and privacy of their Personal Information, nominal damages, and additional losses as described above.

101. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Nationwide and California Class members' Personal Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nationwide and California Class.

102. Nationwide and California Class members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and Nationwide and California Class members of money or property that Defendant may have acquired by means of its unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT IV
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200 – Unfair Business Practices
(On Behalf of Plaintiff and the Nationwide Class,
Or in the Alternative, On Behalf of Plaintiff and the California Class)

103. Plaintiff re-alleges and incorporate by reference herein all of the allegations contained in paragraphs 1 through 70.

104. Defendant engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and

the Nationwide and California Class members' Personal Information with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Nationwide and California Class members' Personal Information in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Nationwide and California Class members. They were likely to deceive the public into believing their Personal Information was securely stored, when it was not. The harm these practices caused to Plaintiff and the Nationwide and California Class members outweighed their utility, if any.

105. Defendant engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the data breach to enact adequate privacy and security measures and protect Nationwide and California Class members' Personal Information from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Nationwide and California Class members. They were likely to deceive the public into believing their Personal Information was securely stored, when it was not. The harm these practices caused to Plaintiff and the Nationwide and California Class members outweighed their utility, if any.

106. As a direct and proximate result of Defendant's acts of unfair practices, Plaintiff and the Nationwide and California Class members were injured and lost money or property, including but not limited to the loss of Nationwide and California Class members' legally protected interest in the confidentiality and privacy of their Personal Information, nominal damages, and additional losses as described above.

107. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Nationwide and California Class members' Personal Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of members of the Nationwide and California Classes.

108. Nationwide and California Class members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and the Nationwide and California Class members of money or property that the Defendant may have acquired by means of their unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of their unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT V
Breach of Implied Contract
(On Behalf of Plaintiff and the Class or, Alternatively, Plaintiff and the California Subclass))

109. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 70.

110. Plaintiff and Class members were required to provide their Personal Information, including names, addresses, Social Security numbers, financial information, beneficiary information, and other personal information to Backroads for tax purposes and to receive employment and benefits.

111. Implicit in the employment agreement between Backroads and its employees was the obligation that Backroads would use the Personal Information of its employees for business purposes only and not make unauthorized disclosures of the information or allow unauthorized access to the information.

112. Additionally, Backroads implicitly promised to retain this Personal Information only under conditions that kept such information secure and confidential and therefore Backroads had a duty to reasonably safeguard and protect the Personal Information of Plaintiff and Class members from unauthorized disclosure or access.

113. Plaintiff and Class members fully performed their obligations under the implied contract with Backroads. Backroads did not.

114. Backroads breached the implied contract with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff's and Class members' Personal Information, which was compromised as a result of the Data Breach.

115. Backroads's acts and omissions have materially affected the intended purpose of the implied contact, which required Plaintiff and Class members to provide their Personal Information in exchange for employment, compensation, and benefits.

116. As a direct and proximate result of Backroads breach of implied contract, Plaintiff and Class members have suffered and will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Personal Information is used; (ii) the publication and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Personal Information, which remains in Backroads possession and is subject to further unauthorized disclosures so long as Backroads fails to undertake appropriate and adequate measures to protect the Personal Information of employees and former employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Personal Information for the rest of their lives.

COUNT VII
Breach of Confidence
(On Behalf Plaintiff and the Class or, Alternatively, Plaintiff and the California Subclass))

117. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 70.

118. At all times during Plaintiff's and Class members' interactions with Backroads, Backroads was fully aware of the confidential and sensitive nature of Plaintiff's and Class members' Personal Information that Plaintiff and Class members provided to Backroads.

119. As alleged herein and above, Backroads' relationship with Plaintiff and Class'

members was governed by expectations that Plaintiff's and Class members' Personal Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

120. Plaintiff and Class members provided their respective Personal Information to Defendant with the explicit and implicit understandings that Backroads would protect and not permit their sensitive Personal Information to be disseminated to any unauthorized parties.

121. Plaintiff and Class members also provided their respective Personal Information to Defendant with the explicit and implicit understanding that Backroads would take precautions to protect that Personal Information from unauthorized disclosure, such as following industry-standard information security practices.

122. Defendant voluntarily received in confidence Plaintiff's and Class members' Personal Information with the understanding that the Personal Information would not be disclosed or disseminated to the public or any unauthorized third parties.

123. Due to Backroads' failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow industry-standard information security practices to secure Plaintiff's and Class members' Personal Information, Plaintiff's and Class members' Personal Information was disclosed to and misappropriated by unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

124. But for Backroads' disclosure of Plaintiff's and Class members' Personal Information in violation of the parties' understanding of confidence, their Personal Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff's and Class members' Personal Information, as well as the resulting damages.

125. As a direct and proximate cause of Backroads' actions and/or omissions, Plaintiff and Class members have suffered damages as alleged herein.

126. The injuries and harm Plaintiff and Class members suffered were the reasonably foreseeable result of Backroads' unauthorized disclosure of Plaintiff's and Class members' Personal Information. Backroads knew its computer systems and technologies for accepting and

securing Plaintiff's and Class members' Personal Information had security vulnerabilities because Backroads knew it was failing to observe industry standard information security practices.

127. As a direct and proximate cause of Backroads' breaches of confidence, Plaintiff and members of the Class have suffered and will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Personal Information is used; (ii) the publication and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Personal Information, which remains in Backroads possession and is subject to further unauthorized disclosures so long as Backroads fails to undertake appropriate and adequate measures to protect the Personal Information of employees and former employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Personal Information for the rest of their lives.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class members, requests judgment against the Defendant and that the Court grant the following:

A. An order certifying the Class, and/or California SubClass, as defined herein, and appointing Plaintiff and his Counsel to represent the Class;

B. An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff's and Class members' Personal Information;

C. An order instructing Defendant to purchase or provide funds for credit

monitoring services for Plaintiff and all Class members;

D. An award of compensatory, statutory, and punitive damages, in an amount to be determined;

E. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: April 26, 2021

Respectfully Submitted,

By: /s/ Michael F. Ram
Michael F. Ram

MICHAEL F. RAM (SBN 104805)
mram@forthepeople.com
MARIE N. APPEL (SBN 187483)
mappel@forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
711 Van Ness Avenue, Suite 500
San Francisco, CA 94102
Telephone: (415) 358-6913
Telephone: (415) 358-6293

JOHN A. YANCHUNIS (*Pro Hac Vice*)
jyanchunis@forthepeople.com
RA O. AMEN (*Pro Hac Vice*)
ramen@ forthepeople.com
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402

Attorneys for Plaintiff